

## REMARKS

This Amendment is in response to the Office Action mailed September 11, 2002. In the Office Action, claims 1-38 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,949,877 (Traw) in view of U.S. Patent No. 6,192,131 (Geer). Applicants respectfully traverse the rejection. The undersigned attorney conducted a telephone conference with the Examiner on November 12, 2002 to discuss the teachings of Traw being inapplicable to the described and claimed operations of the subject application. The undersigned attorney submits herewith a Request for Continued Examination and revised claims per our discussion.

With respect to claims 1, 16 and 33, the Office Action alleges that Traw fails to teach an inventive concept of receiving a revocation list corresponding to a given range of identifiers. However, it is alleged that Geer teaches this inventive concept (see column 5, lines 54-61). Applicants respectfully disagree and respectfully submits that a prima facie case of obviousness has not been established because Geer merely describes a certificate revocation list that identifies the serial numbers of all revoked certificates corresponding to compromised or stolen smart cards. Geer fails to describe either the act of or means for (1) verifying that an identifier of a host device associated with an access module is within a range of host identifiers and/or (2) the act of or means for determining whether the host device associated with the access module is on the revocation list after the identifier of the host device is verified or determine to be within the range of the host identifiers for the revocation list. *See Claim 1 (lines 5-9); claim 16 (lines 5-7); claim 33 (lines 8-12) of the subject application.* Instead, Geer simply teaches scanning of the certificate revocation list without any prior consideration as to identifier boundaries to more quickly ascertain whether a revocation list is applicable to the host device.

With respect to claims 2-3, and 17-18, the Office Action alleges that column 8, lines 32-57 of Traw teaches a method wherein the revocation list is received out band along with the copy

controlled information. Applicants respectfully disagree. As set forth on column 6, lines 48-50 of Traw, the protected content and the certificate revocation list (CRL) are placed on prerecorded media. However, there is no suggestion for supplying the CRL in band as a collective stream of information or out of band through separate mediums. Applicants respectfully request the Examiner to reconsider the rejection.

In addition, the Office Action states that column 2, lines 5-45 of Traw describes the revocation list as being an MPEG private syntax information data structure containing revocation information that is content-specific (claim 4). Applicants respectfully disagree and contend that a prima facie case of obviousness has not been established because column 2, lines 5-45 of Traw is merely general boilerplate language as to term definitions and other terminology.

With respect to claims 9, 12 and 15, it is alleged that column 8, lines 32-57 of Traw describe a method wherein the copy control is denied to the host by not descrambling the copy control content. Such descriptions are not found in this section of the text. Instead, this section of Traw generally relates to the establishment of a content channel without mention of any descrambling operations whatsoever.

With respect to claims 13 and 14, Applicants respectfully submit that Traw does not offer any teachings of an access module being selected from a group consisting of an NRSS-A module, NRSS-B module, Point of Deployment (POD) module and ISO7816 smart card, which performs conditional access by not descrambling the copy control content for the host device and the revocation list. Instead, as mentioned above, column 8, lines 32-57 of Traw generally describe the establishment of a content channel in which a message is sent with the randomly generated key which is unique for each stream of content identification of the symmetric cipher to be used and the isochronous channel associated with the content stream.

With respect to claims 16-20 and 33-38, Applicants respectfully request the Examiner to reconsider the allowability of the claims based on revisions made thereto. Also, consideration of newly added claims 39-47 is respectfully requested.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

1           1.       (Twice Amended) A method for controlling access to copy controlled content to  
2 a host device comprising:  
3           receiving copy controlled content;  
4           receiving a revocation list corresponding to a given range of host identifiers;  
5           verifying that an identifier of a host device associated with an access module is within the  
6 range of host identifiers;  
7           determining whether [a] the host device associated with [an] the access module is on the  
8 revocation list after the identifier of the host device is verified to be within the range of the host  
9 identifiers for the revocation list; and  
10          if the identification of the host device is on the revocation list, causing the associated  
11 access module to deny the copy controlled content to the host device.

1           2.       (Amended) The method of claim 1, wherein the revocation list is received in  
2 band as part of a digital bitstream including [along with] the copy controlled content.

1           3.       (Amended) [The] A method [of claim 1, wherein] comprising:  
2 receiving copy controlled content;  
3 receiving a revocation list corresponding to a given range of host identifiers,  
4 the revocation list is received out of band over a separate channel from a digital bitstream  
5 including [of] the copy controlled content;  
6 determining whether a host device associated with an access module is on the revocation  
7 list; and  
8 if the host device is on the revocation list, causing the associated access module to deny  
9 the copy controlled content to the host device.

1           4.       (Amended) The method of claim [1]3, wherein the revocation list is MPEG  
2 private syntax information data structure.

1           5.       (Amended) The method of claim 1, wherein the receiving of the revocation list  
2 comprises receiving a plurality of revocation lists, where each list corresponds to a given range  
3 of host identifiers.

1           6.       (Twice Amended) The method of claim [1]5, wherein [prior to determining  
2 whether the host device is on the revocation list, the method further comprising reading the  
3 revocation list having the range of host identifiers to] verifying that the identifier of the host  
4 device associated with the access module is [bounded by] within the range of host identifiers  
5 comprises determining which revocation list of the plurality of revocation lists comprises a range  
6 of host identifiers within which the identifier of the host device is bounded.

1           7.       (Amended) The method of claim 1 further comprising allowing access to the  
2 copy controlled content if the host device is not on the revocation list.

1           8.       (Amended) The method of claim 1, wherein [the revocation list contains  
2 revocation information that is content specific] prior to verifying the method further comprises  
3 authenticating the revocation list as having a larger revocation list version number.

1           9.       The method of claim 1, wherein the copy controlled content is denied to the host  
2 device by not descrambling the copy controlled content.

1           10.      The method of claim 1, wherein the host is selected from the group including of a  
2 set top box, television, video player, video recorder, hard disk player, hard disk recorder,  
3 personal computer, memory stick recorder, minidisk player, minidisk recorder, digital video disk  
4 (DVD) player, DVD Recorder, compact disk (CD) player and CD recorder.

1           11.      (Amended) The method of claim 1, wherein the revocation list is transmitted to  
2 devices [could] coupled to a home network, the home network using a communication medium  
3 from one of the group: 1394, Universal Serial Bus, Blue Tooth, and Panel Link.

1           12.     The method of claim 1, wherein the access module performs conditional access  
2 by not descrambling the copy controlled content for the host device on the revocation list.

1           13.     The method of claim 1, wherein the access module denies the copy controlled  
2 content by not outputting the copy controlled content to the host device on the revocation list.

1           14.     The method of claim 12, wherein the access module is selected from the group  
2 consisting of an NRSS-A module, NRSS-B module, Point of Deployment (POD) module, and  
3 ISO7816 smart card.

1           15.     (Amended) The method of claim 1, further comprising [the access module]  
2 conditionally descrambling the copy controlled content [and authenticating a proper revocation  
3 list version number] by the access module if the identifier of the host device is not on the  
4 revocation list.

1           16.     (Twice Amended) An apparatus for controlling access to copy controlled content  
2 to a host device comprising:

3           means for receiving copy controlled content;

4           means for receiving a revocation list corresponding to a range of identifiers;

5           means for determining whether a host device associated with an access module is on the  
6 revocation list [if] after an identifier of the host device is determined to be within the range of  
7 identifiers associated with the revocation list;

8           means for causing the access module to deny the copy controlled content to the host  
9 device if the identifier associated with the host device is on the revocation list.

1           17.     The apparatus of claim 16, wherein the revocation list is received by the access  
2 unit in band along with the copy controlled content.

1           18.     The apparatus of claim 16, wherein the revocation list is received by the access  
2 unit out of band of the copy controlled content.

1           19.    The apparatus of claim 16 further comprising means for descrambling the copy  
2   controlled content if the host device is not on the revocation list.

1           20.    The apparatus of claim 16, wherein the revocation list contains revocation  
2   information that is content specific.

1           21.    (Cancelled).

1           22.    (Cancelled).

1           23.    (Cancelled).

1           24.    (Cancelled).

1           25.    (Cancelled).

1           26.    (Cancelled).

1           27.    (Cancelled).

1           28.    (Cancelled).

1           29.    (Cancelled).

1           30.    (Cancelled).

1           31.    (Cancelled).

1           32.    (Cancelled).

1 21-33. (Amended) A computer readable medium containing instructions, which when  
2 executed by a processing system, [which when executed by a processing system perform a  
3 method for controlling] controls access to copy controlled content [to a host device], the  
4 computer readable medium comprising:  
5 means for receiving a revocation list;  
6 means for receiving a plurality of revocation lists each corresponding to a different range  
7 of host identifiers;  
8 means for determining whether a host device associated with an access module is on the  
9 revocation list by initially verifying whether an identifier of the host device is within a range of  
10 host identifiers associated with one of the plurality of revocation lists, and if so, verifying  
11 whether the identifier of the host device is contained in the one of the plurality of revocation  
12 lists;  
13 [if the host device is on the revocation list,] means for causing the associated access  
14 module to deny the copy controlled content to the host device.

1 22-34. The computer readable medium of claim 33, wherein the revocation list is  
2 received in band along with the copy controlled content.

1 23-35. The computer readable medium of claim 33, wherein the revocation list is  
2 received out of band of the copy controlled content.

1 24-36. (Amended) The computer readable medium of claim 33, [said method further  
2 comprising receiving a plurality of revocation lists, where each list corresponds to a given range  
3 of host identifiers] wherein each of said means for receiving, copy controlled content and said  
4 means for receiving the plurality of revocation lists are executable instructions.

1 25-37. The computer readable medium of claim 33, wherein the copy controlled content  
2 is denied to the host device by not descrambling the copy controlled content.

B



1 ~~26~~ 38. (Amended) The computer readable medium as set forth in claim 33, wherein [the  
2 copy controlled content is not output to the host device if the host device is on the revocation list]  
3 said means for determining and said means for causing are executable instructions.

1 ~~27~~ 39. (New) A device for controlling access to copy controlled content, comprising:  
2 a tuner to tune to a selected frequency for receipt of the copy controlled content;  
3 a demodulator unit coupled to the tuner, the demodulator unit to demodulate the copy  
4 controlled content and output the demodulated copy controlled content; and  
5 an access unit configured to receive the demodulated copy controlled content and a  
6 plurality of revocation lists each corresponding to a different range of host identifiers, the access  
7 unit to determine whether an identifier of the device is within a range of any of the plurality of  
8 revocation lists, and if so, to (i) determine whether the identifier of the device on one of the  
9 plurality of revocation lists and (ii) deny the copy controlled content to the device if the identifier  
10 is listed on one of the plurality of revocation lists.

1 ~~28~~ 40. (New) The device of claim 39, wherein the plurality of revocation lists are  
2 received in band as part of the same digital bistream with the copy controlled content.

1 ~~29~~ 41. (New) The device of claim 39, wherein the plurality of revocation lists are  
2 received out of band being transmitted through a separate medium than the copy controlled  
3 content.

1 ~~30~~ 42. (New) The device of claim 41, wherein the plurality of revocation lists are  
2 received over a telephone line and the copy controlled content is received over either a cable or a  
3 wireless satellite transmission.

1 ~~31~~ 43. (New) The device of claim 39, wherein each of plurality of revocation lists  
2 corresponds to a different group of devices.

1 ~~32~~ 44. (New) The device of claim 39 further comprising a processor coupled to the  
2 access unit.

1 ~~33~~ 45. (New) The device of claim 44, wherein the processor to receive an enhancement  
2 control message, the enhancement control message including a key to descramble the copy  
3 controlled content.

1 ~~34~~ 46. (New) The device of claim 44, wherein the access unit receives the enhancement  
2 control message along with the copy controlled information and the processor transmits  
3 information to the access unit to enable the access unit to locate the enhancement control  
4 message.

1 ~~35~~ 47. (New) The device of claim 46, wherein the enhancement control message  
2 received by the access unit further includes a version number associated with the plurality of  
3 revocation lists.

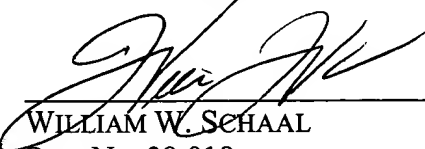
CONCLUSION

In view of the amendments and remarks made above, it is respectfully submitted that all pending claims are in condition for allowance, and such action is respectfully solicited.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: December 11, 2002

  
\_\_\_\_\_  
WILLIAM W. SCHAAL  
Reg. No. 39,018

12400 Wilshire Boulevard, Seventh Floor  
Los Angeles, California 90025  
(714) 557-3800

CERTIFICATE OF MAILING

*I hereby certify that this correspondence is being  
transmitted via facsimile under 37 CFR §1.8 on:  
December 11, 2002.*

  
\_\_\_\_\_  
Corrin R. Reynolds

12/11/02  
Date

B